

Breaking a quantum key distribution system through a timing side channel

Antía Lamas-Linares and Christian Kurtsiefer

Department of Physics, National University of Singapore
2 Science Drive 3, Singapore 117542

antia.lamas@nus.edu.sg

<http://qoptics.quantumlah.org/la/>

Abstract: The security of quantum key distribution relies on the validity of quantum mechanics as a description of nature and on the non-existence of leaky degrees of freedom in the practical implementations. We experimentally demonstrate how, in some implementations, timing information revealed during public discussion between the communicating parties can be used by an eavesdropper to undetectably access a significant portion of the “secret” key.

© 2008 Optical Society of America

OCIS codes: (030.5260) Coherence and statistical optics: photon counting; (270.5290) Quantum optics: photon statistics; (999.9999) Quantum cryptography

References and links

1. M. Dúsek, N. Lütkenhaus, and M. Hendrych, “Quantum Cryptography,” *Prog. in Opt.* **49**, 381–454 (2006).
2. C. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in *Proceedings of the IEEE Int. Conf. On Computer Systems and Signal Processing (ICCSP)*, p. 175 (Bangalore, India, 1984).
3. A. Ekert, “Quantum cryptography based on Bell’s Theorem,” *Phys. Rev. Lett.* **67**, 661–663 (1991).
4. N. Gisin and R. Thew, “Quantum Communication,” *Nature Photonics* **1**, 165–171 (2007).
5. C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster, and J. G. Rarity, “A step towards global key distribution,” *Nature* **419**, 450 (2002).
6. C. Kurtsiefer, P. Zarda, S. Mayer, and H. Weinfurter, “The breakdown flash of Silicon Avalanche Photodiodes - backdoor for eavesdropper attacks?” *J. Mod. Opt.* **48**, 2039–2047 (2001).
7. V. Makarov and D. R. Hjelle, “Faked states attack on quantum cryptosystems,” *J. Mod. Opt.* **52**, 691–705 (2005).
8. V. Makarov, A. Anisimov, and J. Skaar, “Effects of detector efficiency mismatch on security of quantum cryptosystems,” *Phys. Rev. A* **74**, 022313 (2006).
9. N. Gisin, S. Fasel, B. Krauss, H. Zbinden, and G. Ribordy, “Trojan horse attack on quantum key distribution systems,” *Phys. Rev. A* **73**, 022320 (2006).
10. Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, H.-K. Lo, “Experimental demonstration of time-shift attack against practical quantum key distribution systems,” *arXiv:0704.3253v1 [quant-ph]*.
11. R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, “Free-space distribution of entanglement and single photons over 144 km,” *quant-ph/0607182*.
12. A. Poppe, A. Fedrizzi, T. Lorünser, O. Maurhardt, R. Ursin, H. R. Böhm, M. Peev, M. Suda, C. Kurtsiefer, H. Weinfurter, T. Jennewein, and A. Zeilinger, “Practical quantum key distribution with polarization entangled photons,” *Opt. Express* **12**, 3865–3871 (2004).
13. K. J. Resch, M. Lindenthal, B. Blauensteiner, H. R. Böhm, A. Fedrizzi, C. Kurtsiefer, A. Poppe, T. Schmitt-Manderbach, M. Taraba, R. Ursin, P. Walther, H. Weier, H. Weinfurter, and A. Zeilinger, “Distributing entanglement and single photons through an intra-city, free-space quantum channel,” *Opt. Express* **13**, 202–209 (2005).
14. I. Marcikic, A. Lamas-Linares, and C. Kurtsiefer, “Free-space quantum key distribution with entangled photons,” *Appl. Phys. Lett.* **89**, 101122 (2006).

15. C.-Z. Peng, T. Yang, X.-H. Bao, Jun-Zhang, X.-M. Jin, F.-Y. Feng, B. Yang, J. Ying, Q. Zhang, N. Li, B.-L. Tian, and J.-W. Pan, "Experimental free-space distribution of entangled photon pairs over a noisy ground atmosphere of 13km," *Phys. Rev. Lett.* **95**, 030502 (2005).
16. C. H. Bennett, G. Brassard, and J.-M. Robert, "Privacy amplification by public discussion," *SIAM J. Comput.* **17**, 210 (1988).
17. MagiQ Technologies (<http://www.magiqtech.com>) and idQuantique (<http://www.idquantique.com>) offer two of the first commercially available QKD systems.

1. Introduction

Theoretical proofs of the security of quantum key distribution (QKD), are a well developed subfield in quantum communication research (see [1]), both in highly idealized [2, 3] and more realistic scenarios [4]. By construction, these proofs assume that the legitimate parties measurement results are isolated from the environment and thus from an eavesdropper. Comparatively little work has been done studying the possible physical side channels associated with particularities of the physical devices used [5, 6] or possible attacks based on the external manipulation of the expected response of the apparatus [7, 8, 9, 10].

All photon-counting implementations of QKD identify a signal photon from background by measurement of the arrival time at detectors. In an ideal scenario, there can be no correlation between the measurement outcome on the quantum variable (e.g. polarization in the original BB84 proposal), and this publicly exchanged timing information. However, in a recent entanglement based QKD implementation, a pulsed down-conversion source provided photon pairs with a well-defined timing signature [11]. For photon identification, timing information was recorded with a high resolution and communicated to the other side (similar scheme as in [5, 12, 13, 14]). We show that there may be an exploitable correlation between the exchanged timing information and the measurement results in the quantum channel.

2. Time response analysis

A configuration implementing the detection scheme just described is shown in Fig. 1. An incoming photon is randomly directed by a beam splitter towards two possible polarizing beam splitters each of which performs a measurement in one basis (H/V or $45^\circ / -45^\circ$). Finally, there are four possible outcomes of the measurement (two bits of information) of which one bit will be made public. The remaining bit is the raw material for generating the secret key and must be kept secret. Although the optical distance from the entrance of the module to the four detectors differs by less than 1 mm, there is a measurable difference in the timing of the electronic signal from the different possibilities. In order to determine the timing differences between the four single photon detectors, we used an attenuated fraction of a pulse train emitted by a Ti:Sapphire femtosecond laser as a light source (see Fig. 2). Single photon detectors consisted of Silicon Avalanche Photodiodes (type C30902S, Perkin-Elmer), operated in a passively quenched configuration. The breakdown of the avalanche region was converted into a digital pulse signal by a high speed comparator, registering a voltage drop over the measurement resistor $R_M = 100\Omega$ of 150 mV, which has to be compared to a maximal voltage drop across R_M of about 700 mV. The distribution of peak amplitudes for the breakdown signal exhibits a spread below 10% for photodetector event rates of $5000\text{--}6000\text{ s}^{-1}$, and the pulse duration before the comparator is on the order of 2 ns.

We obtained the timing distribution with an oscilloscope sampling at 20 GS/s, by interpolating the time when the comparator output passed through the 50% value between the two logical levels. Time reference is a trigger signal supplied by a MSM Schottky reference photodiode (G7096-03, Hamamatsu) looking at another fraction of the optical pulse train. The timing jitter of 10 ps (FWHM) we observe between consecutive pulses from the mode-locked laser gives an

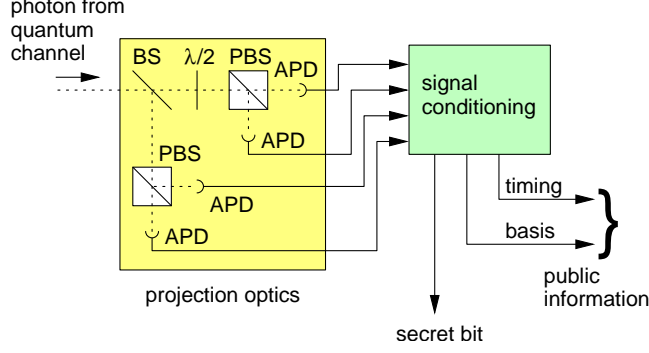


Fig. 1. A typical configuration of photocounting detectors for quantum key distribution. A beam splitter (BS), polarizing beam splitters (PBS) and a half wave plate ($\lambda/2$), divert incoming photons onto a set of detectors, which generate a macroscopic timing signal. This timing information and e.g. a projection basis is revealed publicly, while information on which detector out of two absorbed a photon is the secret used to subsequently generate a key.

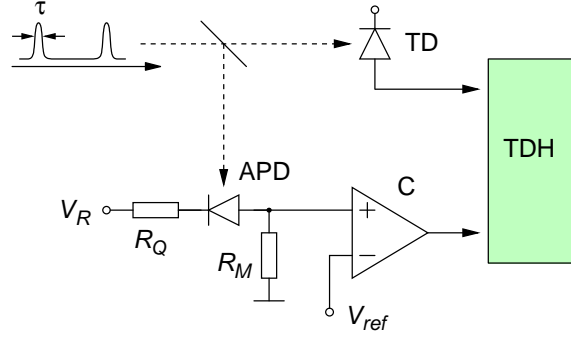


Fig. 2. Experimental set-up to characterize the timing jitter of a single photon detector. A train of ultrashort light pulses from a mode-locked Ti:Sapphire laser is sent with strong attenuation into a passively quenched Si avalanche photodiode (APD). A histogram of timing differences (TDH) with respect to the signal of a trigger photodiode (TD) is recorded.

upper bound for the total timing uncertainty. The resulting timing histograms of the different detectors (Fig. 3) show a clearly different centroid location with respect to the trigger pulse. We model the observed distribution with a convolution product of an exponential decay and a Gaussian distribution,

$$d_i(t) = \frac{1}{2\tau_e} e^{-\frac{t-t_0}{\tau_e}} \cdot e^{-\frac{(t-t_0)^2}{4\tau_G^2}} \operatorname{erfc}\left(\frac{t-t_0}{\tau_G}\right) \quad (1)$$

The fit values for the temporal offset t_0 and the exponential and Gaussian decay constants τ_e , τ_G for the four detectors $i = 1, 2, 3, 4$ are summarized in table 1. While the difference between τ_e and τ_G differ maximally by 38 ps and 20 ps, respectively, the time offsets t_0 can differ up to 240 ps between detectors 2 and 4. The physical origin of this difference could be attributed to differences in the electrical delays for the different detectors on the order of a few cm on the circuit board layouts, and to different absolute pulse heights of the detected breakdown currents due to different parasitic capacities for the different diodes.

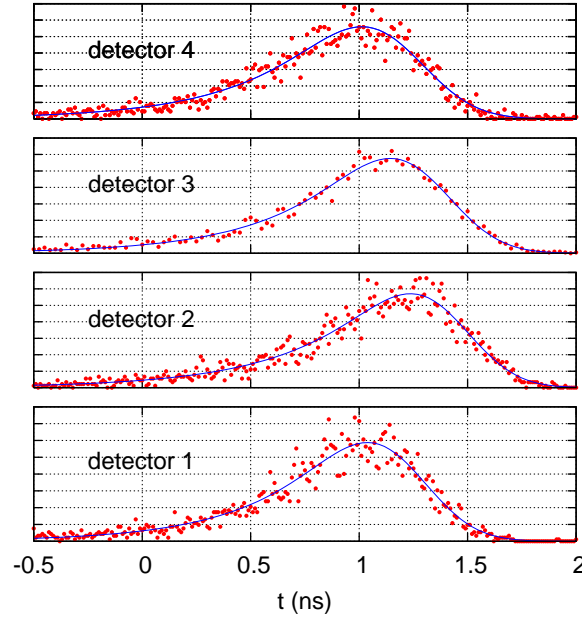


Fig. 3. Photoevent timing histograms for the four detectors involved in a quantum key distribution receiver. While the general shape of the distributions is similar, there is a distinction in the response time visible for detectors 1 and 4 with respect to detectors 2 and 3, which, if not compensated, can be exploited by an eavesdropper to gain knowledge about the measurement result. The solid lines represent a fit to the model in equation 1.

Table 1. Extracted model parameters for the time distributions of the different photodetectors with their statistical uncertainties.

Detector i	t_0 (ps)	τ_e (ps)	τ_G (ps)
1	1138 ± 7	395 ± 7	288 ± 4
2	1356 ± 6	433 ± 7	279 ± 4
3	1248 ± 4	409 ± 5	292 ± 3
4	1117 ± 7	415 ± 7	302 ± 4

3. Information extraction

An eavesdropper can exploit these differences in the detector responses d_i , and obtain information on the secret key by listening in the publicly communicated detection times. The knowledge in principle attainable by the eavesdropper is quantified by the mutual information $I(X; T)$ between the time distribution of detector clicks (publicly revealed) and the bits composing the secret key:

$$I(X; T) = H(X) + H(T) - H(X, T) \quad (2)$$

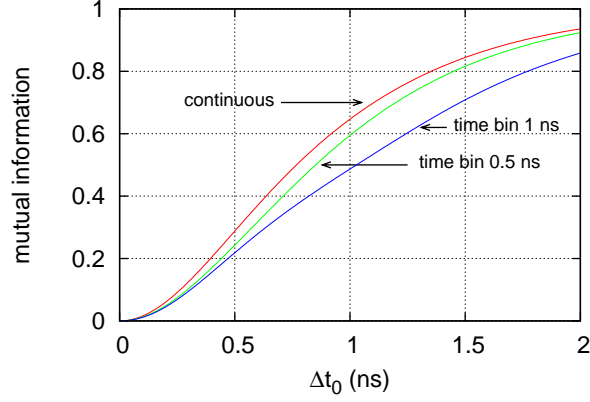


Fig. 4. Eavesdropper's information on the secret bit as a function of delay Δt_0 between detector timing distributions with identical shapes. The three curves represent different levels of discretization of the data. The top curve corresponds to the continuous distribution and the subsequent are for 0.5 ns and 1 ns time bins. As expected, with an increasing time bin there is less information available for the eavesdropper. For Δt_0 as small as 0.5 ns the eavesdropper will gain access to more than a quarter of the “secret key”.

There, X represents the distribution of logical 0 and 1, and T is the distribution of detection times. The entropies and joint entropies of the distributions are given by

$$\begin{aligned}
 H(T) &= - \int \bar{d}(t) \log_2[\bar{d}(t)] dt \\
 H(X) &= - \sum_x p^0(x) \log_2[p^0(x)] \\
 H(X, T) &= - \sum_x \int p(x, t) \log_2[p(x, t)] dt \\
 &= - \sum_x \int p^0(x) d_x(t) \log_2[p^0(x) d_x(t)] dt
 \end{aligned}$$

where $\bar{d}(t) = \sum_x p^0(x) d_x(t)$ is the probability of a click occurring at time t for the ensemble of detectors, and $d_x(t)$ the probabilities of a click at a particular time t for a detector corresponding to logical value $x \in \{0, 1\}$. In most protocols, the prior distribution of logical values is balanced such that $p^0(0) = p^0(1) = 0.5$.

If we bin the detector results in the manner most favorable to the eavesdropper by assigning detectors (1,2) to one basis, (3,4) to the other basis, and taking detectors groups (1, 3) and (2, 4) to represent 0 and 1, the average extractable information is $3.8 \pm 0.38\%$. It is worth considering in detail how the distinguishability of the distributions comes about, and how quickly the eavesdropper knowledge of the key changes. Figure 4 shows the eavesdropper's knowledge of the secret bit for two distributions $d_0(t), d_1(t)$ with the same $\tau_e = 400$ ps, $\tau_G = 290$ ps, but with different relative delays Δt_0 . Detectors that are uncompensated by as little as $\Delta t_0 = 500$ ps will give the eavesdropper access to more than 25% of the “secret” key. Since a small relative delay is not visible in the usual experimental setups which employ coincidence windows between 1 and 20 ns [12, 13, 15, 14], it requires an additional effort to make sure that this leakage channel is closed.

The solution to this particular side channel is not complex, the timing information should

be characterized and the delays equalized, randomized or the precision truncated such that the potential information leakage is below a certain threshold. Quantum cryptography protocols can then deal with this in the same way they deal with errors, by applying an appropriate amount of privacy amplification [16]. In every real experiment the timing information is communicated with a finite precision that could be adjusted for this purpose. Figure 4 shows the effect of discretizing the time information into 0.5 ns and 1 ns time bins (a typical experimental value of ≈ 150 ps gives a negligible difference with the continuous distribution). As expected, the eavesdropper’s information is reduced as the bin width increases. Somewhat counterintuitively there is still a strong leakage even at bin sizes comparable to the width of the distribution $d(t)$; furthermore there is a penalty in the form of increased background. For our particular device, the main distinguishing feature is the time offset. If this is compensated for (i.e. made identical for all detectors), and applying the same procedure as before to obtain the leakage to an eavesdropper given the probability distributions, we find the leakage to be around 0.3%.

It is reasonable to ask whether this problem affects “prepare and measure” protocols as well. A typical BB84 QKD system based on weak coherent pulses has a synchronous operation, and the detector side will locally determine whether the detected event falls in the right part of the timing frame to be counted as genuine. This binary decision will not provide information to the eavesdropper from the detector side. However, the problem has just been displaced from the detectors to the emitters: if the states to be sent are prepared by different physical devices, their temporal response needs to be characterized, and the possible information leakage should be evaluated with a similar analysis.

4. Conclusions

Quantum cryptography is slowly leaving the purely academic environment and starting to appear in commercial products [17]. The theoretical aspects of its security are a very active research area but comparatively little has been done in terms of scrutinizing the practical systems. However, there is increasing interest in looking at the side channels arising from the physical realization in practical systems (see recent work by Zhao et al. [10] for an attack on a commercial product based on a proposal by Makarov et al. [8]). We have shown here how some of the information publicly revealed by the communicating parties in reasonable mature implementations, may lead to a large proportion of the key becoming insecure.

Acknowledgements

The authors thank Artur Ekert for useful discussions. This work was partly funded by DSTA in Singapore.